CCPOA visitor and incident coordination proposal

Prepared for Century City Property Owners Association
Veyra proposal for discussion
24 November 2026

Decision requested

We propose that CCPOA support the design of a governed pilot connecting willing buildings and existing access providers to a shared visitor and incident service. The initial decision would authorise scoping and governance work. Live sharing of personal incident information would follow only after the lawful model and any required regulatory authorisation are in place.

The problem to address

The operational concern is recurring disruption from short-term rental groups that return under a different booking holder. Building-level action against one lead guest may leave other participating properties without relevant information. The proposal addresses that gap by verifying actual guests and retaining properly reviewed incident outcomes.

The proposed CCPOA component

The proposed free, open-source component would support a controlled central repository for participating building and unit records, visitor registrations and incident cases. Owners and building systems would submit relevant information. Security teams would record interventions and outcomes. Designated reviewers would manage findings and permitted alerts.

Third-party systems, including providers such as ATG, could participate through documented APIs. This is a proposed integration opportunity and does not imply a partnership or confirmed technical compatibility. Open-source code would not make personal records publicly accessible.

Initial scope

The pilot would focus on short-term stays and their visitors. The wider model could later support long-term tenants, staff, contractors and commercial visitors through separate rules appropriate to their circumstances and access rights.

The operational workflow

Owner authorisation

The owner or authorised managing agent identifies the unit, stay dates, intended guests, contact person and backup. The system records permission for the stay and sends relevant registration information to the building and CCPOA service.

Arrival and individual access

Security checks each arrival against the authorised guest list. The agreed identity-verification method links returning guests to their existing record and allows correction of false matches. Individual access passes expire with the permitted visit. Additional day visitors follow the building approval process.

Intervention and follow-up

The guard records the complaint separately from observed facts, contacts the unit, records the requested action and follows up. The record captures cooperation, recurrence, evidence and the final outcome. Serious safety concerns follow the emergency process immediately.

Review and subsequent checks

A designated reviewer assesses evidence and individual involvement. A later permitted check can return a restricted alert about a relevant substantiated incident. An authorised person makes and records any resulting decision under agreed policy.

Example of a noise complaint

A resident reports loud music. Security contacts the unit and requests lower volume. If the guests comply and security confirms the disturbance has ended, the case records “resolved after intervention”. If the noise continues or returns, security records each intervention and escalates the case. Multiple complaints about one event attach to the same incident.

A booking links the people relevant to an investigation. It does not establish that every guest committed an infringement. Individual consequences require evidence of involvement. Pending reports remain distinguishable from substantiated findings.

Pilot capabilities and responsibilities

- Guest and visitor registration with owner authorisation and arrival verification.
- Individual access passes linked to the approved building, permitted areas and visit period.
- Owner and managing-agent escalation with an agreed response deadline and backup contact.
- Guided incident handling with evidence, cooperation, review outcomes and shift handover.
- Unit-level reporting on recurring substantiated incidents, incomplete registrations and owner response times.

Proposed responsibilities

CCPOA would convene the participating parties, agree shared rules and nominate the people responsible for governance. The precise legal roles, hosting arrangements and authority to make decisions must be established before live operation.

Owners and managing agents would authorise stays, maintain guest information and respond to escalations. Security teams would verify arrivals and record observations accurately. Reviewers would investigate, determine outcomes within their authority and manage disputes. Technology providers would integrate within their approved permissions.

Restricted API participation

Each provider would receive credentials and permissions limited to its authorised functions and building relationships. Interfaces would support permitted registration updates, incident submissions and narrowly scoped verification responses. General database browsing or bulk access to personal histories would not form part of ordinary provider access.

The technical design should include access logs, provider onboarding and revocation, encryption, safeguards against repeated identity probing, and controls to prevent duplicate records or incidents. Reporter updates should preserve a version history. Only authorised reviewers should change findings or review outcomes.

Operating costs

The proposed core is free and open source. Hosting, support, integrations, hardware, identity verification, training and legal work still require an agreed budget and accountable parties. This proposal does not commit CCPOA or a provider to funding, pricing or a delivery date.

Privacy and fair decision making

POPIA requires a lawful basis and safeguards for each processing purpose. Registration terms or a broad consent checkbox do not by themselves authorise unrestricted sharing. The design must address minimal data collection, notices, accuracy, security, retention and the rights of individuals to access or challenge their records. [1]

Processing criminal, unlawful or objectionable conduct on behalf of third parties may trigger prior authorisation under section 57. A South African privacy lawyer should assess the proposed model, applicable exceptions and regulatory process before such processing begins. Criminal-behaviour information and automated adverse decisions also raise specific POPIA requirements. [1, 2]

Case status and reputation

The pilot should use understandable case statuses rather than a numerical reputation score. “New or no history” is neutral. An incident record should distinguish a report under review, a resolved intervention and a substantiated incident requiring review. Absence of complaints is not proof of good behaviour.

If numerical scoring is explored later, stakeholders must first agree evidence standards, weighting, retention, expiry, appeals and safeguards against unfair outcomes. Association with a booking or group alone should not determine a person’s status. Adverse outcomes should receive human review.

Pilot stages and measures

First, agree governance, legal requirements, operating costs and participating buildings. Next, test registration, matching, permissions and incident workflows with synthetic records. Begin a limited live pilot only once the necessary approvals and controls are in place. Review results before considering wider participation.

Agree acceptance targets in advance. Measures should include registration completeness, false-match corrections, owner response times, incident resolution, substantiated recurrence, disputed records and guard workload. A small pilot can establish usability and data quality but cannot prove precinct-wide crime reduction.

Later development

Disclosed noise-level alerts and emergency visitor accounting are possible later additions. Noise alerts should prompt verification. An emergency list should clearly distinguish registered guests from recorded check-ins and should not be treated as a guaranteed live occupancy count. [3, 4]

Decisions for the pilot workshop

- Who holds responsibility for each dataset, investigation and access decision?
- Which buildings and providers will participate, and which integrations are feasible?
- What identity evidence is necessary, and how will false matches and outages be handled?
- Which incidents justify cross-property alerts, to whom and for how long?
- How will individuals receive notice, challenge records and seek review?
- Who funds and operates hosting, support, training and legal work?
- What evidence will determine whether the pilot should continue or expand?

References

1 Protection of Personal Information Act 4 of 2013

Relevant provisions include sections 1, 10–11, 14, 16, 18–24, 26–33, 57–58 and 71.

https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013popi.pdf

2 Information Regulator prior authorisation

Regulatory process and guidance.

https://inforegulator.org.za/prior-authorisation/

3 Minut noise monitoring

International example of alerts for sustained noise. Product capability is not a local legal clearance.

https://support.minut.com/en/articles/3714389-noise-monitoring

4 Envoy visitor evacuation tools

International example of signed-in visitor lists and emergency notifications.

https://envoy.help/en/articles/3444474-using-visitors-for-evacuation

Sources checked 23 November 2026. The operational problem and CCPOA context reflect the project brief. All service capabilities and governance arrangements described here are proposals for discussion.